The Fortified Inbox

April 2007

epsilon

Insight

Today's email users are more aware, have more tools at their disposal, and are taking action to protect themselves from spam, spyware and phishing. Email marketers should embrace their growing role in corporate security initiatives, and leverage state-of-the-art best practices and technology to distinguish their communications, enhance consumer safety and comfort, and maximize revenue and ROI.

Epsilon surveyed 430 email users about their attitudes and behaviors related to email and spam. We asked several questions designed to gain insight into how they felt about the safety and security of their inboxes.

Consumers Demand Delivery of Expected Email

Email users are expressing increased reliance on the channel and are taking proactive measures to ensure receipt of wanted and critical communications.

- **Most actively protect legitimate email from spam filters' false positives.** Sixty five percent sometimes or always add legitimate, trusted senders to their address books, and 58 percent sometimes or always check their spam or junk folders for misdirected messages.

- **And they demand receipt of important communications.** Seventy percent would consider switching their ISP/email client ("mailbox provider") if they did not receive "critical communications for example order confirmations, billing statements, etc." This compares to the 47 percent who, when asked a similar question in October 2003, told us they'd consider switching their mailbox provider if they "did not receive critical communications" from their "primary credit card issuer due to a filtering/blocking mistake."[1]

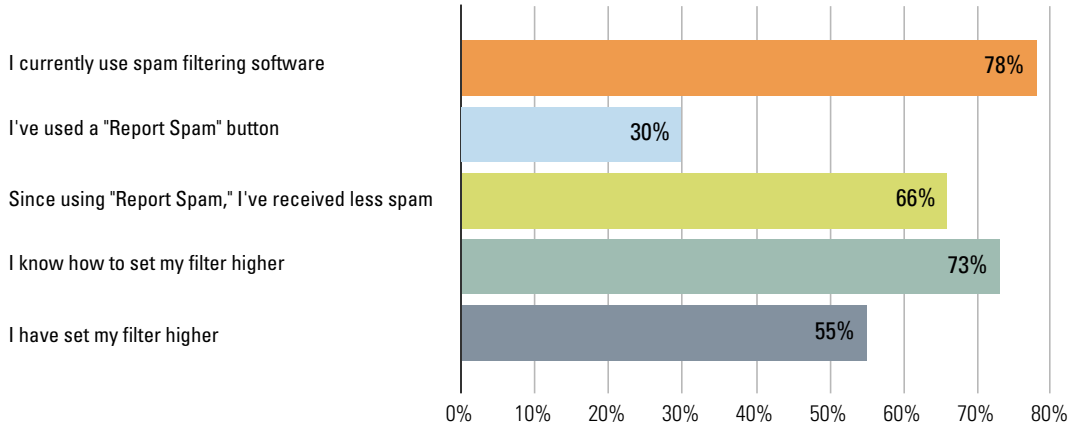
Taking Filtering into their Own Hands

Email users are also more aware of the potential threats they face in their inboxes, and are using and customizing spam filters to suit their individual needs and preferences.

- **They're aggressively using – and fine tuning – spam filters.** Seventy-eight percent say they currently use anti-spam filtering software, about the same as last year, but up from 68 percent in February 2005. Seventy-three percent know how to change their anti-spam filters' default settings, and 55 percent have set their filters to be more aggressive than the default settings originally established by their mailbox provider.

- **They're clicking "Report Spam" buttons… and the buttons are working.** Nearly a third (30 percent) are clicking "Report Spam" buttons or links, and two-thirds of those who do say taking such action reduces the amount of spam they receive.

Figure 1: Consumers Taking Control of the Inbox



1 Epsilon/RoperASW NOP World Research, October 2003

epsilon

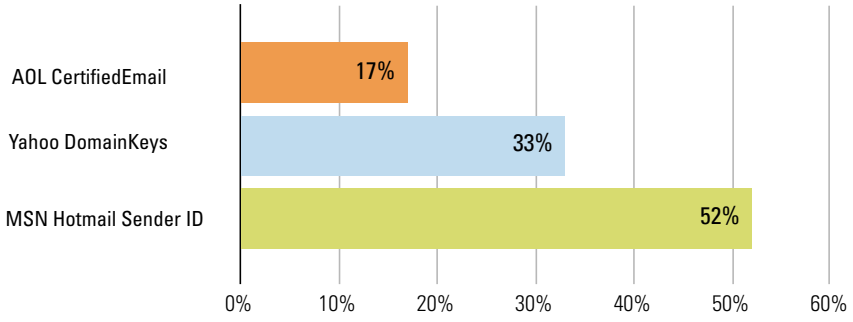
Awareness of Visual Legitimacy Cues

Collaborative industry initiatives including authentication, accreditation and reputation (AAR) are helping mailbox providers more effectively distinguish good email from bad. Consumers are also starting to notice AAR-based visual legitimacy cues displayed at some of the most popular mailbox providers.

- **A growing number of Yahoo users are noticing DomainKeys confirmations.** One-third recently noticed these confirmations, up from the one-in-five who said they did a year ago.[2]
- **Half of MSN/Hotmail users are aware of Sender ID.** Fifty-two percent of MSN and Hotmail users recently noticed a warning telling them "The sender of this message could not be verified by Sender ID."[3]
- **Few have received CertifiedEmail.** Fewer than one-in-six AOL users recently noticed an icon in their browser indicating that a message they received was CertifiedEmail.[4]

Marketers should continue to pay close attention to developments in the AAR space, including increasingly pervasive visual legitimacy cues. In particular, they should study how these alerts may affect consumers' email experience, their impact on confidence and trust, and ultimately their consequences for response and ROI.

Figure 2: Consumer Awareness of Visual Legitimacy Cues



2 Base (2007): 84 Yahoo users; Base (2006): 117.
3 Base (2007): 64 MSN/Hotmail users.
4 Base (2007): 61 AOL users.

epsilon

Email Users: More Aware, Less Afflicted

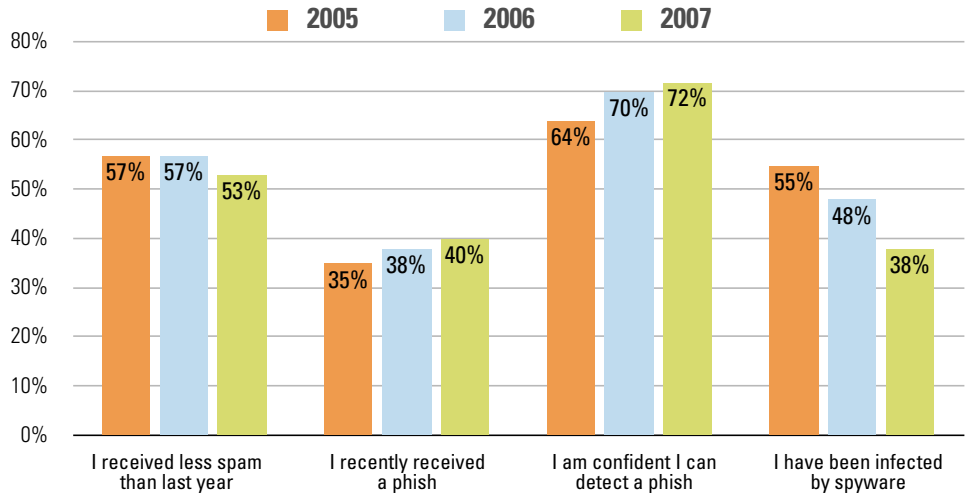
Against this backdrop of growing consumer awareness, action, and technical innovation, consumers are becoming less affected by email borne nuisances and threats.

- **2007 marks the third consecutive year in which the majority received less spam than the year before.** Fifty-three percent say that the amount of spam they received over the past year decreased. Although the raw volume of spam circulating the Internet may remain high, leading mailbox providers including AOL and Microsoft maintain that they are becoming better at reducing the amount actually routed to end users.

- **Most believe they can spot a phish before being reeled in.** Industry, government agencies and media outlets continue to beef up online safety education and awareness efforts, and consumer confidence in the ability to detect phishing is high and growing. Seventy two percent say they can identify a phish today, compared to 64 percent in February 2005.

- **Fewer report spyware infections.** The widespread availability of free spyware blocking software and built-in browser protection tools is helping reduce the problem, and we continue to see dramatic year-over-year declines in the number of consumers reporting that their computers have been infected. When we first asked this question in February 2005, more than half – 55 percent – told us they'd been "infected by spyware that caused pop-up ads on my computer, hijacked my browser start pages or pages, and altered important system files." That number dropped to 48 percent in January 2006, and now sits at 38 percent.

Figure 3: More Confident, Better Protected Against Email Borne Threats



epsilon

Strategic Marketers Will Thrive Behind Fortified Walls

Marketers should keep proper perspective: the vast majority of fraud and information breaches occur through traditional, offline channels, while phishing and the Internet still account for only small pieces of the pie.[5] Meanwhile, great strides continue to be made in further securing email and enhancing the channel's ability to thrive as a vehicle for commerce, communication and education.

But keep in mind that as times change and technologies evolve, so will the nature of the threats facing firms and their customers. As consumers continue to interact with, and conduct commerce through a constantly evolving and diverse media and communications landscape, keeping them safe will become evermore core to the pitch and a bedrock necessity for business success.

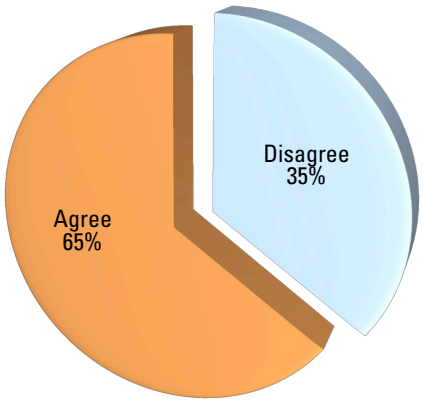
Marketers will continue to find themselves inexorably involved in overall corporate anti-fraud and customer safety initiatives, and the best among them will coordinate and extend these efforts across multiple channels and consumer touchpoints.

To get welcomed into (and thrive behind) the walls of the fortified inbox, marketers should:

- **Emphasize consumer control. Now more than ever, it must be your number one priority.** Your own subscribers can damage your reputation and threaten your delivery rates and folder placement by complaining instead of simply opting out. A growing number of consumers are clicking Report Spam buttons, at the same time that a high and growing number are equating clicking these buttons with unsubscribing (65 percent agree "when I click on the 'Report Spam' button I am unsubscribing from the email," compared to 55 percent last year). They aren't clicking "Report Spam" because they don't know how to opt-out – quite to the contrary, today's savvy email users are clicking these buttons because they are finding them simple to use and highly effective at preventing the receipt of future unwanted communications.

  To help avoid complaints, make strong privacy commitments and follow up on them. Clearly and conspicuously explain to subscribers how their personal information will be used, shared and protected, and convey the choices they have - especially as it relates to their ability to quickly, easily and effectively opt-out at any time during registration, on your web site, and in all subsequent email communications.

Figure 4: Most Equate Clicking "Report Spam" With Unsubscribing



"When I click 'Report Spam' I am unsubscribing from the message"

5 Javelin Strategy & Research, 2007 Identity Fraud Survey Report, February 2007.

epsilon

- **Implement multiple authentication solutions.** Adopt multiple layers of email authentication, including IP-based solutions like SPF/Sender ID and cryptography-based ones like DomainKeys/DKIM, to help protect users from fraudulent and spoofed messaging, and to instill greater confidence in the growing number of consumers who are noticing and reacting to authentication-based visual legitimacy cues across popular mailbox providers like Yahoo and MSN/Hotmail. Verify with internal IT staff and external providers that all authentication compliance is accurate and up-to-date. Also study the effects of emerging fee-based accreditation/reputation solutions on consumer trust and response, and consider testing these programs for select communications.

- **Anticipate and respond to the effects of consumers' setting their filters higher.** Test rendering and deliverability across the largest mailbox providers you send email to *under the highest filtering settings* prior to deployment. With consumers setting their spam filters to more aggressive levels, the implications for marketers can be significant: Delivery optimization will dictate strict adherence to technology, privacy and database marketing best practices more than ever before. And this also highlights the growing need to adjust creative templates for optimal rendering in the event of image blocking. For example, under default settings, the beta version of the largest mailbox provider, Yahoo Mail, will render images automatically if marketers are listed in the end users "contacts"/address book or are CertifiedEmail senders. However, if a user sets his filter to the highest settings, images won't render in any messages, even in communications received from certified and contacts-listed senders.

- **Educate – don't terrify – users about email safety.** Education, awareness, and new technologies continue to better protect consumers from online threats, as we see with increased confidence in the ability to identify phishing, and declining reports of spyware infections. There is no need to raise consumers' alertness level to a persistent "code red," but marketers do have a responsibility to develop an understanding of the unique threats consumers might face when interacting with their brand via email, and to arm them with sufficient knowledge to protect themselves. Build email and online safety education pages or centers on your web site which contain practical, easy-to-understand advice geared towards a mass audience of consumers. Highlight the availability of this information with prominent links on your web site and in the footer of all email communications. Cater to consumers' multi-channel engagement, and, as appropriate, consider including email safety information in print statement stuffers, as leaflets at retail locations, when they sign up through call centers, and elsewhere.

- **Help users recognize legitimate email.** The education job doesn't end with warning consumers about threats. Today's marketers should also take steps to ensure that increasingly confident email users do not accidentally mistake legitimate communications for phishing. Develop branding and structural guidelines for email headers and templates that emphasize consistency so that recipients will recognize and trust messages. In addition, marketers' registration pages should include links to samples of recent email newsletters so that subscribers learn what their authentic messaging looks like.

- **Recruit users to actively protect legitimate email.** Though consumer use of email address books is high, only 43 percent say that the companies they do business with usually request to be added to address books — a figure unchanged over the past three years. Request "add to address book" during registration and in subsequent communications, and provide instructions for how to do so across various popular mailbox providers. In addition, educate subscribers about the potential for spam filtering false positives and inform them when collecting their email addresses that some mailbox providers might accidentally block or route legitimate email to junk folders.

- **Take a 360 degree view of consumers and your interactions with them.** Email communications should not exist in a silo. The best marketers take a holistic view of their consumer interactions, and are prepared to respond to their needs – and concerns – across all channels. Call center representatives, for example, should be empowered with tools to automatically retrieve email communications sent to individual customers in order to verify their authenticity. One large Epsilon client in the financial sector logged nearly 3,000 unique queries to such an email verification system in just the first five months since its launch. The result: Not only were some of these customers better protected from potential threats, but as one senior marketing executive at the firm told us: "Advisors can now confirm to card members that we did in fact send them a particular marketing email and turn a discussion about phishing into a sales discussion about the product."

About Epsilon

Through our combination of client-centric marketing solutions, Epsilon helps leading companies understand, manage, measure and optimize their customer relationships and grow their marketing ROI. Since 1969, Epsilon has developed innovative marketing solutions that not only meet our client needs but also exceed expectations through a thorough understanding of the market and our client's customers. Today, Epsilon is distinguished in the marketplace as the only provider to be ranked a leader in both The Forrester Wave: Database Marketing Service Providers, Q1 2006 and The Forrester Wave: Email Marketing Service Providers, Q4, 2005.

For more information, contact
Epsilon
info@epsilon.com
(212) 995-7500
www.epsilon.com

Customer Insight Realized.™

epsilon